The worm that turned on the US

By John Feffer

The Pentagon has traditionally presented cyber-war as "their hackers" against "our defenders". Out there, especially in China, a faceless horde of anonymous computer users are arrayed against the United States in an updated version of the "yellow peril".

In 2010, the Pentagon complained publicly for the first time about the Chinese government deploying civilian hackers to go after US targets. These cyber-attacks date back at least to 1999 when, after the North Atlantic Treaty Organization (NATO) bombed the Chinese Embassy in Belgrade, Chinese hackers launched a slew of "denial of service" attacks that, among other results, shut down the White House website for three days.

According to the experts, we're suffering death by a thousand

hacks. In his book America the Vulnerable, Joel Brenner starts out the introductory chapter by bemoaning the Chinese download of 20 terabytes of information from the Defense Department in an infamous maneuver from several years ago.

"To carry this volume of documents in paper form, you'd need a line of moving vans stretching from the Pentagon to the Chinese freighters docked in Baltimore harbor fifty miles [80 kilometers] away. If the Chinese tried to do that, we'd have the National Guard out in 15 minutes. But when they did it electronically, hardly anyone noticed."

Brenner doesn't address whether the Chinese actually found anything useful in that enormous data dump, nor does the former senior counsel at the National Security Agency talk about what the United States has stolen from the Chinese. Threat, after all, sells books (as well as high-priced intelligence programs and weapon systems).

Washington is not just worried about Beijing. The US government loses sleep over Russians, al-Qaeda sympathizers and even disgruntled computer nerds on the home front. US authorities have vigorously pursued Anonymous, the hacker tribe that has targeted corporate websites unfriendly to the Occupy movement and to WikiLeaks.

There's a reason it's called the Defense Department and not the War Office. Listen to Washington and you'd think the United States was simply a healthy body under attack by a legion of foreign microbes in league with traitorous parasites within. But several major news stories over the past week paint a very different picture of the US government approach to cyber-war. It turns out that our hands are not clean at all.

The Barack Obama administration indirectly confirmed last week, through a leak in The New York Times, that it had teamed up with Israel to create Stuxnet, the worm that burrowed into Iran's nuclear program and created havoc in its uranium-enrichment centrifuges.

More disturbing perhaps has been the administration's attempts to extend "full-spectrum dominance" to the cyber-world. We might sound all defensive. But in fact we've been quite offensive in our actions.

The Stuxnet worm, part of a secret US program codenamed Olympic Games, was initially a George W Bush administration effort. As he passed the presidential baton onto Obama, Bush urged his successor to preserve two programs: the Olympic Games and the drone attacks in Pakistan.

Obama complied on both. The virus was intended to instruct Iranian centrifuges to essentially destroy themselves. In 2010, however, the bug jumped from the Natanz facility in Iran to the Internet, where it began to replicate wildly, a programming error that Obama aides blamed on their Israeli partners. Still, the bug remained anonymous, and Washington pushed ahead with the program. Eventually, a new version of Stuxnet damaged one-fifth of Iran's centrifuges, setting back the program for an unknown period of time.

The Obama administration has apparently approved this leak, for it has not issued any denials. Going into the autumn elections, Obama the presidential candidate wants to make sure that the Republicans can't charge him with appeasing Iran. Stuxnet is the cyber equivalent of assassinating Osama bin Laden: a mission that demonstrates that the Obama administration is daring, is willing to break rules and play dirty, and operates as if the world is a video game and Americans have special powers.

But Stuxnet also raises certain expectations. "Some officials question why the same techniques have not been used more aggressively against North Korea," David Sanger writes in his investigative report. "Others see chances to disrupt Chinese military plans, forces in Syria on the way to suppress the uprising there, and Qaeda operations around the world."

The Pentagon may have already used these techniques against the competition. For two years, the Pentagon's Cyber Command has been overseeing the development of various cyber weapons, a process that has recently been fast-tracked. And the administration just announced its effort to crowd-source cyber warfare through "Plan X".

The $110-million program will solicit proposals from universities and video-game manufacturers. Plan X's parent agency, the Defense Advanced Research Projects Agency (DARPA), is reportedly shifting its cyber-efforts from the defensive to the offensive.

Since the end of the Cold War, the United States has tried to sustain its singular superpower status through "full spectrum dominance". Such dominance, according to the Joint Vision 2020 from those pre-9/11 days of June 2000, means "the ability of US forces, operating alone or with allies, to defeat any adversary and control any situation across the range of military operation".

The spectrum has included cyber-space for some time. Offensive cyber-tactics fall into five basic categories: using the Internet to win hearts and minds; denial of service attacks that effectively paralyze websites; electronic attacks on infrastructure such as nuclear power plants; sabotage through the sale of defective hardware or software; and operational attacks that accompany conventional battle plans, as when Israel disabled Syrian radar systems when it bombed a suspected nuclear weapons facility in 2007.

Hackers have long realized that even sophisticated systems have backdoors. The United States is slowly waking up to the realization that its basic infrastructure - power plants, waste-treatment facilities, indeed anything controlled by a computer - is vulnerable to hostile take-over.

The search engine Shodan shows all the different computers you can access online. "One researcher using the system," according to a recent Washington Post story, "found that a nuclear particle accelerator at the University of California at Berkeley was linked to the Internet with virtually no security."

I can imagine a group of hackers over at Fort Meade that the National Security Agency pays handsomely to map all the vulnerable points in the infrastructure of other countries. Even as the United States scrambles to patch its own leaks, it is no doubt making plans to breach the cyber-Maginot Lines of its adversaries.

All's fair in love and war, you might say. But we ramp up our e-offensive at no inconsiderable risk to ourselves. Our cyber-attacks, as with any offensive strategy, can provoke retaliation. Sanger concludes his Stuxnet investigation with a cautionary note: "It is only a matter of time, most experts believe, before [the United States] becomes the target of the same kind of weapon that the Americans have used, secretly, against Iran."

Retaliation, in this case, comes with a twist. Ordinary citizens can't send their own unmanned aerial vehicles to the United States. But some ordinary citizens can leverage the power of the Internet to hack into US sites and cause considerable damage.

Also, if we attack infrastructure, civilians are at heightened risk. Knocking out centrifuges is one thing. But cyber-warriors could just as easily target the entire electricity grid. "You could argue that out of the gate cyber-war is going to be war crimes," says Marcus Ranum of Tenable Network Security.

"If you're talking taking out an electronic infrastructure preparatory to a ground attack, you're talking about shutting down their hospitals and shutting down their businesses, shutting down their stock exchange, shutting down their street lights, and screwing people's lives up. These are all contrary to the civilized laws of how wars are supposed to be fought."

The prospect of such attacks taking out US infrastructure has prompted Richard Clarke, in his new book Cyber War, to propose a ban on cyber-attacks on civilian targets.

And, finally, the most frightening possibility is the worm that goes out of control. Stuxnet did some damage outside Iran but it was relatively tame as malware goes. But more serious stuff is now out there - see, for example, Flame - and who knows what's in the pipeline that could, like a cyber-smallpox, cause a major e-pandemic?

We are creating genetically engineered life forms. We are considering geo-engineering on a massive scale to avert global warming. And now we are inching closer to importing the MAD (mutually assured destruction) logic of nuclear weapons into cyber-space.

Remember: the Internet was originally a creation of DARPA (with a minor assist from Al Gore). Now DARPA, like Darth Vader, is attempting to reclaim its progeny and recruit it to the dark side. Where are the light sabers to fend it off?

The more things change

Perhaps the greatest fallout from the Stuxnet program is diplomatic. "This will certainly play into [Iran's] fears about what else is out there," a former intelligence official told The Washington Post. "It certainly won't make them eager to get back to the negotiating table."

And indeed, the latest round of negotiations with Iran has gone nowhere. "The chief reason for the failure of the talks was the unwillingness of the West to even consider what Iran has sought the most: scaling back existing sanctions and imposing a freeze on pending European Union (EU) and American sanctions against Iran's financial and energy sectors," writes Foreign Policy In Focus contributor Richard Heydarian in "Dashed Hopes for Baghdad Breakthrough".

"Unless the West is willing to negotiate concessions with regard to its punitive sanctions, the Iranians will continue to push the frontiers of enrichment, thus further raising the prospects for an armed confrontation."

The US Congress, meanwhile, is back to its same old tricks on the Middle East. "Earlier this month," writes FPIF senior analyst Stephen Zunes in "Bipartisan Assault on Middle East Peace", "the House of Representatives passed a dangerous piece of legislation [HR 4133] that would undermine the Israeli-Palestinian peace process, weaken Israeli moderates and peace advocates, undercut international law, further militarize the Middle East, and make Israel ever more dependent on the United States."

In Egypt, meanwhile, the first round of the presidential elections produced two frontrunners: a candidate from the Muslim Brotherhood and a candidate of the old regime. "The upcoming run-off is a contest between the remnants of the Mubarak regime and the Islamist Muslim Brotherhood, continuing a struggle now waged for more than 60 years," write FPIF contributors Bonnie Bricker and Adil Shamoo in "Egypt's Path Winds toward Democracy".

"The old regime is associated with a vast security apparatus and its dictatorial, corrupt, and abusive tactics, along with its concentration of wealth among a small number of well-connected and influential families. On the other side, the Muslim Brotherhood promotes social justice, using Islamic principles to guide governance. Under the Muslim Brotherhood, however, women and minority rights could be curtailed, and democratic principles may not be fully applied."

For a lively account of how Egypt got to where it is today, check out FPIF Pick of the week, The Journey to Tahrir, which FPIF contributor Melissa Moskowitz calls a "deep and meaningful portrait of the revolution that shocked the world".

Secrets and lies

Reporter David Axe recently found himself in a middle of a controversy when he reported the comments of Army Brigadier General Neil Tolley that US Special Forces were on the ground in North Korea gathering intelligence.

"Almost immediately, the Pentagon repudiated the story," writes FPIF contributor Tim Shorrock in Tall Tale about Special Forces in North Korea? "A spokesman for US Forces in Korea told Voice of America that Axe's quotes were 'made up'. A Pentagon flack later added that the general's comments 'were distorted [and] misreported.' Axe, who wrote a good-humored account of his experience on his blog, War is Boring, stuck to his story and asked the Pentagon for an apology."

It turns out that the general was speaking hypothetically. But the United States has certainly gone to great lengths to acquire human intelligence inside North Korea. "The United States has also relied on the information gathered by its ally, South Korea, from the network of spies that it ran in North Korea," I write in Spying on the North, a column for Hankyoreh newspaper.

"These bukpagongjakwon formed an elite army Intelligence Unit tasked with intelligence-gathering, infiltration, and even assassination. North Korea's incursions in South Korea are well-known: the attack on the Blue House in 1968, the submarine that ran aground in 1996, the numerous spies that have infiltrated South Korean society. But South Korea's missions have been no less extensive and audacious. One infamous group of ex-cons, trained on Shilmido to assassinate Kim Il-sung in the wake of the 1968 Blue House incursion, revolted against their guard-trainers and made their way to Seoul to petition the president. None survived, and the incident was suppressed."

On the topic of secrecy, the Trans Pacific Partnership (TPP) is continuing to meet in closed-door sessions. "Nine countries are currently negotiating the TPP: the United States, Australia, New Zealand, Chile, Peru, Brunei, Vietnam, Malaysia, and Singapore," writes FPIF contributor Arnie Saiki in Japan, Nuclear Energy and the TPP.

"Despite large protests at home against accession into the TPP negotiations, Japan, Canada and Mexico are also expected to join. Although the negotiations are being held in secret, leaked documents confirm that contrary to democratic practice, the documents connected to the negotiations will remain secret for four years after being signed or dismissed."

Deepening democracy

Many women leaders have come to the fore in Latin America: Laura Chinchilla in Costa Rica, Dilma Rousseff in Brazil, Cristina Fernandez in Argentina. "Currently, however, the presence of women in politics is more symbolic than anything else," writes FPIF guest columnist Erika Guevara-Rosas in Rocky Road to Gender Equality in Latin America.

"These new women leaders are not transforming their societies in fundamental ways. Indeed, the feminization of politics in the region has not yet translated into the incorporation of feminist and women's rights agendas, or even into improved conditions for the majority of women."

Rebecca McKinnon's new book Consent of the Networked documents the efforts of activists to use the Internet to get around government censorship. "New products like Tor, which enables users to upload and download without being traced, are becoming popular in places like China, Iran and Egypt," writes FPIF contributor Julia Heath in her review.

"Diaspora, Crabgrass, FreedomBox and StatusNet are decentralized social media platforms that provide users local control and anonymity, which makes them better suited for activists."

John Feffer is co-director of Foreign Policy In Focus at the Institute for Policy Studies.